



PERÚ

Ministerio
de Educación

Secretaría General

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la Esperanza y el Fortalecimiento de la Democracia"

Lima, 27 de marzo de 2026

OFICIO N.º 00599-2026-MINEDU/SG

Señora Congresista

ARIANA ORUÉ MEDINA

Presidenta de la Comisión de Ciencia, Innovación y Tecnología

Congreso de la República

Presente.-

Asunto: Opinión sobre el Texto Sustitutorio del Dictamen recaído en los Proyectos de Ley N°13415/2025-CR y 13511/2025-CR.

Referencia: a) Oficio Múltiple N°D000157-2026-PCM-SC
b) Oficio N°00144-PO-2025-2026-CCIT-AMOM-CR
c) Oficio N°00148-PO-2025-2026-CCIT-AMOM-CR
d) Oficio N°00155-PO-2025-2026-CCIT-AMOM-CR

De mi mayor consideración:

Es grato dirigirme a usted, por especial encargo de la señora Ministra de Educación, a fin de saludarla cordialmente y en atención a los documentos de la referencia, mediante los cuales se solicita opinión respecto a las siguientes iniciativas legislativas:

- Proyecto de Ley N°13415/2025-CR, "Ley que declara el 3 de diciembre de cada año, como el "Día Nacional de la Ciberseguridad".
- Proyecto de Ley N°13511/2025-CR, "Ley que declara el Día Nacional de la Seguridad Informática- Ciberseguridad el 3 de diciembre de todos los años".

Al respecto, sírvase encontrar adjunto para conocimiento y fines correspondientes el Informe N° 00430-2026-MINEDU/SG-OGAJ, elaborado por la Oficina General de Asesoría Jurídica del Ministerio de Educación, mediante el cual se emite informe sobre el Texto Sustitutorio del Dictamen recaído en los Proyectos Ley N°13415/2025-CR y 13511/2025-CR, en virtud del cual se propone la "Ley que declara Día Nacional de la Ciberseguridad el 30 de noviembre de cada año".

Hago propicia la oportunidad para expresarle las muestras de mi especial consideración.

Atentamente,



GAVILANO IGLESIAS Doris
Lorena FAU 20131370998
hard

SECRETARIA GENERAL
Consejo de Ministros
Soy el autor del documento
2026/03/27 16:36:55

CC: Secretaría de Coordinación de la Presidencia y Consejo de Ministros

MDP2026-EXT-180554, 180530 y 195764
LGI/cztl

EXPEDIENTE: MPD2026-EXT-0180554 CLAVE: 66AF11

Esto es una copia auténtica imprimible de un documento electrónico archivado en el Ministerio de Educación, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web:

https://esinad.minedu.gob.pe/e_sinadmed_5VDD_ConsultaDocumento.aspx

www.gob.pe/minedu

Calle Del Comercio 193
San Borja, Lima 41, Perú
T: (511)615 5800

Documento electrónico firmado digitalmente en el marco de la Ley N° 27269, Ley de Firmas y Certificados Digitales, su Reglamento y modificatorias. La integridad del documento y la autenticidad de la(s) firma(s) pueden ser verificadas en <https://apps.firmaperu.gob.pe/web/validador.xhtml>





PERÚ

Ministerio
de Educación

Secretaría General

Oficina General de
Asesoría Jurídica

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la Esperanza y el Fortalecimiento de la Democracia"

INFORME N.º 00430-2026-MINEDU/SG-OGAJ

A : **DORIS LORENA GAVILANO IGLESIAS**
SECRETARIA GENERAL

De : **CLAUDIA MABEL ZANINI FERNÁNDEZ**
JEFA DE LA OFICINA GENERAL DE ASESORÍA JURÍDICA

Asunto : OPINIÓN SOBRE EL DICTAMEN FAVORABLE RECAÍDO EN LOS PROYECTOS DE LEY 13415/2025-CR Y 13511/2025-CR, POR EL CUAL, CON TEXTO SUSTITUTORIO, SE PROPONE LA "LEY QUE DECLARA DÍA NACIONAL DE LA CIBERSEGURIDAD EL 30 DE NOVIEMBRE DE CADA AÑO".

Referencia : a) OFICIO N° 00155-PO-2025-2026-CCIT-AMOM-CR
b) OFICIO N° 00148-PO-2025-2026-CCIT-AMOM-CR
c) OFICIO N° 00144-PO-2025-2026-CCIT-AMOM-CR
d) OFICIO MÚLTIPLE N° D000157-2026-PCM-SC
e) INFORME N° 00142-2026-MINDEU/VMGP-DITE
f) INFORME TÉCNICO N° 00033-2026-MINEDU/SPE-OTIC-UCSI
g) OFICIO N° 00142-2026-MINEDU/SPE-OPEP-UPP
Expediente MDP2026-EXT-0180554
Expediente MDP2026-EXT-0180530
Expediente MDP2026-EXT-0195764

Fecha : Lima, 24 de marzo de 2026

Tengo el agrado de dirigirme a usted, en atención al asunto del rubro y a los documentos de la referencia, para informarle lo siguiente:

I. ANTECEDENTES:

- 1.1. Mediante el Oficio N° 00155-PO-2025-2026-CCIT-AMOM-CR, la presidenta de la Comisión de Ciencia, Innovación y Tecnología del Congreso de la República, solicita opinión al Ministerio de Educación (en adelante, **MINEDU**) respecto del Proyecto de Ley N° 13511/2025-CR (en adelante, **Proyecto de Ley**).
- 1.2. Con fecha 10 de marzo de 2026, la mencionada comisión aprueba el Texto Sustitutorio de la "LEY QUE DECLARA DÍA NACIONAL DE LA CIBERSEGURIDAD EL 30 DE NOVIEMBRE DE CADA AÑO" (en adelante, el Texto Sustitutorio), derivado de los siguientes proyectos de Ley:
 - PL 13415/2025-CR, LEY QUE DECLARA EL 3 DE DICIEMBRE DE CADA AÑO, COMO EL "DÍA NACIONAL DE LA CIBERSEGURIDAD"¹.

¹ Solicitud de la Comisión de Ciencia, Innovación y Tecnología del Congreso de la República sobre el PL 13415/2025-CR tramitada bajo SINAD MDP2026-EXT-0180530. Asimismo, mediante Oficio Múltiple N° D000157-2026-PCM-SC, la Secretaría de Coordinación de la presidencia del Consejo de Ministros, trasladó al MINEDU la solicitud de opinión sobre el PL 13415/2025-CR de

EXPEDIENTE: MPD2026-EXT-0180554 CLAVE: 56EBA4

Esto es una copia auténtica imprimible de un documento electrónico archivado en el Ministerio de Educación, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web:

https://esinad.minedu.gob.pe/e_sinadmed_3VDD_ConsultaDocumento.aspx

www.gob.pe/minedu

Calle Del Comercio 193
San Borja, Lima 41, Perú
T: (511)615 5800





PERÚ

Ministerio
de Educación

Secretaría General

Oficina General de
Asesoría Jurídica

- **PL 13511/2025-CR, LEY QUE DECLARA EL DÍA NACIONAL DE LA SEGURIDAD INFORMÁTICA – CIBERSEGURIDAD EL 3 DE DICIEMBRE DE TODOS LOS AÑOS.**

- 1.3. Con Informe N° 00142-2026-MINEDU/VMGP-DITE, la Dirección de Innovación Tecnológica en Educación (en adelante, **DITE**) dependiente del Viceministerio de Gestión Pedagógica (en adelante, **VMGP**), manifiesta que carece de competencia para evaluar el Proyecto de Ley, toda vez que la iniciativa no contempla actividades curriculares que deban ser ejecutadas por el Sector Educación, como tampoco incorpora el “Día Nacional de Seguridad Informática – Ciberseguridad” en el Calendario Cívico Escolar.
- 1.4. A través del Informe Técnico N° 00033-2026-MINEDU/SPE-OTIC-UCSI, la Unidad de Calidad y Seguridad de la Información (**UCSI**), dependiente de la Oficina de Tecnologías de la Información y Comunicación (en adelante, **OTIC**) de la Secretaría de Planificación Estratégica (en adelante, **SPE**), opina sobre la propuesta legislativa.
- 1.5. Mediante Oficio N° 00142-2026-MINEDU/SPE-OPEP-UPP, la Unidad de Planificación y Presupuesto (en adelante, **UPP**), dependiente de la Oficina de Planificación Estratégica y Presupuesto (**OPEP**) de la SPE, manifiesta que no le corresponde emitir opinión sobre el Proyecto de Ley, por no corresponder en materias de los sistemas de Planeamiento Estratégico y Presupuesto Público.

II. ANÁLISIS:

Respecto a las funciones de la Oficina General de Asesoría Jurídica

- 2.1 Conforme con el literal g) del artículo 65 del Reglamento de Organización y Funciones del Minedu, aprobado por Decreto Supremo N° 001-2015-MINEDU, corresponde a esta Oficina General emitir opinión jurídica respecto de los proyectos y autógrafas de Ley.
- 2.2 Es importante precisar que el presente informe contiene el análisis técnico y legal sobre el Proyecto de Ley, siendo que sus conclusiones responden a la solicitud de opinión formulada por el Congreso de la República en el ejercicio de su función legislativa.

Sobre el contenido del Texto Sustitutorio

- 2.3 El Texto Sustitutorio presenta el siguiente contenido:

“Artículo único. Día Nacional de la Ciberseguridad

Se declara Día Nacional de la Ciberseguridad el 30 de noviembre de cada año, con la finalidad de concientizar a la población, a las organizaciones de la sociedad civil y a las instituciones gubernamentales y privadas sobre la importancia de proteger la información”.

Opinión técnica de la Oficina de Tecnologías de la Información y Comunicación

- 2.4 Mediante Informe Técnico N° 00033-2026-MINEDU/SPE-OTIC-UCSI, la UCSI señala lo siguiente sobre el Proyecto de Ley:

la Comisión de Ciencia, Innovación y Tecnología del Congreso de la República, tramitada bajo SINAD MDP2026-EXT-0195764.

EXPEDIENTE: MPD2026-EXT-0180554

CLAVE: 56EBA4

Esto es una copia auténtica imprimible de un documento electrónico archivado en el Ministerio de Educación, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web:

https://esinad.minedu.gob.pe/e_sinadmed_3VDD_ConsultaDocumento.aspx

www.gob.pe/minedu

Calle Del Comercio 193
San Borja, Lima 41, Perú
T: (511)615 5800





- a. El Proyecto de Ley tiene como objetivo declarar el Día Nacional de la Seguridad Informática – Ciberseguridad, con la finalidad de que el Estado concientice a las personas y organizaciones la importancia de ejercer buenas prácticas de seguridad al utilizar computadoras, Internet, o cualquier otro medio de almacenamiento de información.
- b. Actualmente, el MINEDU a través de la UCSI y en coordinación con el Comité de Gobierno y Transformación Digital, se encuentra implementando el Sistema de Gestión de Seguridad de la Información, el cual es un proceso de mejora continua basado en la NTP ISO/IEC 27011:2022.
- c. Dentro de las actividades del referido Comité, se encuentra programada la concientización sobre seguridad de la información a nivel institucional, asegurando que el personal y las partes interesadas, desarrollen las competencias necesarias para mitigar riesgos y proteger los activos críticos de información de la entidad.
- d. En ese sentido, para la UCSI, la propuesta normativa resulta congruente y complementaria con los esfuerzos institucionales, pues la institucionalización de una fecha conmemorativa fortalecerá la cultura digital en la población, facilitando la adopción de medidas preventivas ante las crecientes amenazas en el ciberespacio.

Opinión legal de la Oficina General de Asesoría Jurídica

- 2.5 Al respecto, el artículo 107 de la Constitución Política del Perú² señala que el Presidente de la República y los Congresistas tienen derecho a iniciativa en la formación de leyes.
- 2.6 En concordancia con la Constitución, el artículo 67 del Reglamento del Congreso de la República (en adelante, **Reglamento del Congreso**)³ menciona que los proyectos de ley son instrumentos mediante los cuales se ejerce el derecho de iniciativa legislativa y se promueve el procedimiento legislativo, con la finalidad de alcanzar la aprobación de una ley por el Congreso.
- 2.7 Asimismo, el artículo 69 del Reglamento del Congreso dispone que los pedidos efectuados por los Congresistas son proposiciones mediante las cuales ejercen su derecho de pedir la información que consideren necesaria a los Ministros y otras autoridades y órganos de la administración, a efecto de lograr el esclarecimiento de hechos o tener elementos de juicio para tomar decisiones adecuadas en el ejercicio de sus funciones⁴.

² **Constitución Política del Perú**
Artículo 107.- El Presidente de la República y los Congresistas tienen derecho a iniciativa en la formación de leyes.

³ **Texto Único Ordenado del Reglamento del Congreso de la República**
Artículo 67.- Las propuestas o proyectos de ley o de resolución legislativa son instrumentos mediante los cuales se ejerce el derecho de iniciativa legislativa y se promueve el procedimiento legislativo, con la finalidad de alcanzar la aprobación de una ley o resolución legislativa por el Congreso.

⁴ **Texto Único Ordenado del Reglamento del Congreso de la República**
Artículo 69.- Los pedidos son proposiciones mediante las cuales los Congresistas ejercen su derecho de pedir la información que consideren necesaria a los Ministros y otras autoridades y órganos de la administración, a efecto de lograr el esclarecimiento de hechos o tener elementos de juicio para tomar decisiones adecuadas en el ejercicio de sus funciones.

Asimismo, los pedidos escritos se pueden efectuar para hacer sugerencias sobre la atención de los servicios públicos.

EXPEDIENTE: MPD2026-EXT-0180554 CLAVE: 56EBA4

Esto es una copia auténtica imprimible de un documento electrónico archivado en el Ministerio de Educación, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web:

https://esinad.minedu.gob.pe/e_sinadmed_3VDD_ConsultaDocumento.aspx

www.gob.pe/minedu

Calle Del Comercio 193
San Borja, Lima 41, Perú
T: (511)615 5800



- 2.8 De acuerdo con lo establecido en el artículo 87 del Reglamento del Congreso⁵, cualquier congresista puede solicitar a los organismos del sector público los informes que estime necesarios para el ejercicio de su función, el cual deberá ser atendido en un plazo de quince (15) días hábiles.
- 2.9 En el presente caso, el Proyecto de Ley tiene como objeto declarar el Día Nacional de la Ciberseguridad el 30 de noviembre de cada año, con la finalidad de concientizar a la población, a las organizaciones de la sociedad civil y a las instituciones gubernamentales y privadas sobre la importancia de proteger la información.
- 2.10 Sobre el particular, considerando las opiniones de la DITE y la UPP, se advierte que el MINEDU carece de competencia para emitir pronunciamiento de fondo sobre la viabilidad del Proyecto de Ley.
- 2.11 En efecto, la materia que se pretende regular carece de cualquier mandato operativo, pedagógico o sectorial dirigido al sistema educativo. Al tratarse de una norma de carácter puramente declarativo orientada a la concientización general de la sociedad y de las instituciones del Estado, su alcance no altera, no regula ni impacta en el diseño de políticas educativas, la gestión escolar ni la currícula nacional. Por tanto, evaluar la viabilidad o pertinencia de esta conmemoración excede el ámbito de las competencias funcionales del Ministerio de Educación.
- 2.12 De otro lado, cabe tener en cuenta que de acuerdo con el artículo 8 del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, *“la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital, es el ente rector en materia de gobierno digital que comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital. Dicta las normas y establece los procedimientos en materia de gobierno digital y, es responsable de su operación y correcto funcionamiento”*.
- 2.13 En ese contexto, al estar enfocada la propuesta normativa en la protección de datos, la integridad de las infraestructuras digitales y la promoción de una cultura de seguridad de la información a nivel nacional, la rectoría técnica e institucional recae de manera exclusiva en la PCM como ente rector del Sistema Nacional de Transformación Digital. Es a dicha entidad a quien le corresponde emitir opinión y

5

Texto Único Ordenado del Reglamento del Congreso de la República

Artículo 87.- Cualquier congresista puede pedir a los ministros, al Jurado Nacional de Elecciones, al contralor general, al Banco Central de Reserva, a la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, a los gobiernos regionales y locales y a todos los demás organismos del sector público, los informes que estime necesarios para el ejercicio de su función. Esta atribución no autoriza a solicitar información sobre procesos judiciales en trámite, salvo que sea pública o el juez o fiscal o la Sala que conoce el asunto acceda a entregar la información, bajo su responsabilidad y siempre que se lo permitan las leyes orgánicas del Poder Judicial y del Ministerio Público y las normas procesales vigentes.

El pedido se hace por escrito fundamentado y preciso. El congresista obligatoriamente debe dirigir copia del oficio conteniendo el pedido a la Mesa Directiva. Si dentro de los quince días posteriores los titulares referidos en el primer párrafo o el funcionario requerido no responden o se niegan a responder, la Mesa Directiva procede a la reiteración del pedido. Transcurridos siete días después de la reiteración, el ministro, el gobernador regional, el alcalde, el titular de la entidad correspondiente o el funcionario requerido está obligado a responder personalmente, según corresponda y lo determine el Consejo Directivo, ante el Pleno o ante la comisión ordinaria, vinculada con el asunto motivo del pedido, bajo responsabilidad, conforme a ley. Mensualmente, se publica la relación de los ministerios, gobiernos regionales, alcaldías o entidades de la administración que hubieren incumplido con responder. Las respuestas a los pedidos de información son suscritas por el titular de la entidad.(...)*

* Artículo modificado por el Artículo Único de la Resolución Legislativa del Congreso N° 001-2023-2024-CR, publicada el 29 septiembre 2023.

EXPEDIENTE: MPD2026-EXT-0180554

CLAVE: 56EBA4

Esto es una copia auténtica imprimible de un documento electrónico archivado en el Ministerio de Educación, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web:

https://esinad.minedu.gob.pe/e_sinadmed_3VDD_ConsultaDocumento.aspx

www.gob.pe/minedu

Calle Del Comercio 193
San Borja, Lima 41, Perú
T: (511)615 5800





PERÚ

Ministerio
de Educación

Secretaría General

Oficina General de
Asesoría Jurídica

evaluar la pertinencia de establecer el 30 de noviembre como una efeméride oficial sobre ciberseguridad.

- 2.14 Sin perjuicio de lo mencionado anteriormente, es importante mencionar que la OTIC, en coordinación con el Comité de Gobierno y Transformación Digital, se encuentra implementando el Sistema de Gestión de Seguridad de la Información bajo las disposiciones de la NTP ISO/IEC 27011:2022. Asimismo, dentro de las actividades del referido Comité, se encuentra la concientización sobre seguridad de la información a nivel institucional.

III. CONCLUSIÓN:

En el marco de competencias del MINEDU, y considerando lo señalado por la DITE, UPP y OTIC se verifica que este Ministerio carece de competencia para evaluar la viabilidad del Texto Sustitutorio, considerando que la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, en su calidad de ente rector en materia de gobierno digital es la autoridad responsable de la seguridad digital.

IV. RECOMENDACIÓN:

Se recomienda dar respuesta a la Comisión de Ciencia, Innovación y Tecnología del Congreso de la República; con copia a la Secretaría de Coordinación de la Presidencia del Consejo de Ministros, en función a la solicitud de opinión.

Es todo cuanto debo informar.

Atentamente,



ZANINI FERNANDEZ
Claudia Mabel FAU
20131370998 hard
JEFA DE LA OFICINA
GENERAL DE ASESORIA
JURIDICA - MINEDU
En señal de conformidad
2026/03/24 16:26:32



Firmado digitalmente por:
ABARCA GARCIA Jorge Luis
FAU 20131370998 soft
Motivo: Doy V° B°
Fecha: 24/03/2026 16:13:08-0500

EXPEDIENTE: MPD2026-EXT-0180554 CLAVE: 56EBA4

Esto es una copia auténtica imprimible de un documento electrónico archivado en el Ministerio de Educación, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web:

https://esinad.minedu.gob.pe/e_sinadmed_3VDD_ConsultaDocumento.aspx

www.gob.pe/minedu

Calle Del Comercio 193
San Borja, Lima 41, Perú
T: (511)615 5800





PERÚ

Presidencia
del Consejo de Ministros

Secretaría General

Secretaría de Coordinación



Firmado digitalmente por PASTOR
PAREDES Milagritos Pilar FAU
2016899926 soft
Cargo: Secretaria De La Secretaria
De Coordinación
Motivo: Soy el autor del documento
Fecha: 16.02.2026 10:03:22 -05:00

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
Año de la Esperanza y el Fortalecimiento de la Democracia

Miraflores, 16 de Febrero del 2026

OFICIO MULTIPLE N° D000157-2026-PCM-SC

Señor (as):

ROGER PAVLETICH VIDAL RAMOS

Secretario General

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

ROSARIO RIOFRÍO ESPINOZA

Secretaria General

MINISTERIO DE ECONOMÍA Y FINANZAS

DORIS LORENA GAVILANO IGLESIAS

Secretaria General

MINISTERIO DE EDUCACIÓN

Presente.-

Asunto : Solicita opinión sobre el Proyecto de Ley N° 13415/2025-CR.

Referencia : a) Oficio N° 00144-PO-2025-2026-CCIT-AMOM-CR
b) Memorando N° D000415-2026-PCM-OGAJ
Expediente 2025-0014023

De mi mayor consideración:

Tengo el agrado de dirigirme a usted con relación al documento de la referencia a), a través del cual la Presidencia de la Comisión de Ciencia, Innovación y Tecnología del Congreso de la República, solicita opinión técnico legal del Proyecto de Ley N° 13415/2025-CR, "Ley que declara el 3 de diciembre de cada año, como el Día Nacional de la Ciberseguridad".

Al respecto, de acuerdo al documento de la referencia b), debido a la materia regulada por el Proyecto de Ley N° 13415/2025-CR, corresponde a su representada emitir opinión en el marco de sus competencias.

En relación al párrafo anterior, se solicita que, emitida la opinión sectorial, ésta sea remitida directamente a la Presidencia de la Comisión de Ciencia, Innovación y Tecnología del Congreso de la República, con copia a la Presidencia del Consejo de Ministros.

Atentamente,

Documento firmado digitalmente

MILAGRITOS PILAR PASTOR PAREDES
SECRETARIA DE LA SECRETARÍA DE COORDINACIÓN
PRESIDENCIA DEL CONSEJO DE MINISTROS

EXPEDIENTE: «2026-0014023»



Esta es una copia auténtica imprimible de un documento electrónico archivado en la Presidencia del Consejo de Ministros, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web:

Url: <https://sgdc Ciudadano.pcm.gob.pe/register/verifica>

Código de Verificación: 0161 7887 5275 4589

**¡EL PERÚ A TODA
MÁQUINA!**



PERÚ

Presidencia
del Consejo de Ministros

Secretaría General

Oficina General de Asesoría
Jurídica



Firmado digitalmente por PEÑARES
FLORES Hugo Alejandro FAU
2016899926 soft
Cargo: Jefe De La Oficina General De
Asesoría Jurídica
Motivo: Soy el autor del documento
Fecha: 12.02.2026 19:27:31 -05:00

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
Año de la Esperanza y el Fortalecimiento de la Democracia

Lima, 12 de Febrero del 2026

MEMORANDO N° D000415-2026-PCM-OGAJ

Para : **MILAGRITOS PILAR PASTOR PAREDES**
SECRETARIA DE LA SECRETARÍA DE COORDINACIÓN
SECRETARÍA DE COORDINACIÓN

De : **HUGO ALEJANDRO PEÑARES FLORES**
JEFE DE LA OFICINA GENERAL DE ASESORÍA JURÍDICA
OFICINA GENERAL DE ASESORÍA JURÍDICA

Asunto : Solicita trasladar pedido de opinión técnico legal y/o sugerencias, respecto del Proyecto de Ley 13415/2025-CR, Ley que propone establecer el 3 de Diciembre de cada año como el "Día Nacional de la Ciberseguridad".

Referencia : OFICIO N° 00144 - PO - 2025 - 2026-CCIT-AMOM-CR

Fecha Elaboración: Lima, 12 de febrero de 2026

Tengo el agrado de dirigirme a su Despacho en atención al Oficio de la referencia, a través del cual la Presidencia de la Comisión de Ciencia, Innovación y Tecnología solicita opinión sobre el Proyecto de Ley N° 13415/2025-CR, Ley que propone establecer el 3 de Diciembre de cada año como el "Día Nacional de la Ciberseguridad".

Al respecto, el referido Proyecto de Ley contiene materias que se encuentran dentro del ámbito de competencia de la Autoridad Nacional del Servicio Civil-SERVIR. En tal sentido, se solicita a su Despacho tenga a bien realizar las gestiones pertinentes ante la citada entidad pública con relación a la iniciativa legislativa señalada, a fin de que pueda remitir su opinión técnico legal a esta Oficina General de Asesoría Jurídica en **un plazo máximo de diez (10) días hábiles**, de modo que, podamos dar respuesta oportuna a la mencionada comisión congresal.

Asimismo, el referido Proyecto de Ley contiene materias que se encuentran dentro del ámbito de competencia del Ministerio de Justicia y Derechos Humanos, Ministerio de Economía y Finanzas y Ministerio de Educación, por lo que se solicita se traslade a dichos Ministerios el pedido de opinión formulado por la Comisión de Ciencia, Innovación y Tecnología del Congreso de la República, precisando que las opiniones que se emitan sean remitidas directamente a la referida Comisión Congresal.

Atentamente,

Documento firmado digitalmente

HUGO ALEJANDRO PEÑARES FLORES
JEFE DE LA OFICINA GENERAL DE ASESORÍA JURÍDICA
OFICINA GENERAL DE ASESORÍA JURÍDICA

HPF/nfu

EXPEDIENTE: 2026-0014023

**¡EL PERÚ A TODA
MÁQUINA!**

Lima, 20 de enero de 2026

OFICIO N° 00144 - PO - 2025 - 2026-CCIT-AMOM-CR

Señor

ERNESTO JULIO ÁLVAREZ MIRANDA

Presidente del Consejo de Ministros – PCM

Jirón Carabaya Cdra. 1 s/n, Palacio de Gobierno

Lima-Centro.-

De mi consideración:

Es grato dirigirme a usted para saludarlo cordialmente, y en la oportunidad solicitar se sirva remitir opinión técnico legal y/o sugerencias, respecto del **Proyecto de Ley 13415-2025-CR, PROPONE ESTABLECER EL 3 DE DICIEMBRE DE CADA AÑO, COMO EL "DÍA NACIONAL DE LA CIBERSEGURIDAD", CON EL PROPÓSITO DE PROMOVER LA PROTECCIÓN DE LOS DATOS PERSONALES, LA INTEGRIDAD DE LAS INFRAESTRUCTURAS DIGITALES Y, LA CONFIANZA EN EL USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC).**

Este pedido se formula, al amparo de lo dispuesto en el artículo 96 de la Constitución Política del Perú, y en los artículos 22, literal b), 69 y 87 del Reglamento del Congreso de la República.

El plazo para la remisión de la opinión respectiva no deberá ser mayor a los quince días útiles de recibido el presente documento. Asimismo, Su opinión será de valioso aporte a la comisión que presido, coadyuvando al resultado de este, por lo que agradeceré sus importantes comentarios a la brevedad posible.

El proyecto de ley mencionado para estudio y análisis por su institución podrá ser descargado en el siguiente link: [pdf](#)

Hago propicia la ocasión para testimoniarle las muestras de mi especial consideración y estima personal.

Atentamente,



Firmado digitalmente por:
ORUÉ MEDINA Ariana Maybee
FAU 20161749126 soft
Motivo: Soy el autor del
documento
Fecha: 22/01/2026 06:48:41-0500

ARIANA MAYBEE ORUÉ MEDINA
Presidenta
Comisión de Ciencia, Innovación y Tecnología

AMOM/ica

Lima, 20 de enero de 2026

OFICIO N° 00148 - PO - 2025 - 2026-CCIT-AMOM-CR

Señor
JORGE EDUARDO FIGUEROA GUZMÁN
Ministro de Educación (MINEDU)
Calle El Comercio N° 193
San Borja.-

De mi consideración:

Es grato dirigirme a usted para saludarlo cordialmente, y en la oportunidad solicitar se sirva remitir opinión técnico legal y/o sugerencias, respecto del **Proyecto de Ley 13415-2025-CR, PROPONE ESTABLECER EL 3 DE DICIEMBRE DE CADA AÑO, COMO EL "DÍA NACIONAL DE LA CIBERSEGURIDAD", CON EL PROPÓSITO DE PROMOVER LA PROTECCIÓN DE LOS DATOS PERSONALES, LA INTEGRIDAD DE LAS INFRAESTRUCTURAS DIGITALES Y, LA CONFIANZA EN EL USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC).**

Este pedido se formula, al amparo de lo dispuesto en el artículo 96 de la Constitución Política del Perú, y en los artículos 22, literal b), 69 y 87 del Reglamento del Congreso de la República.

El plazo para la remisión de la opinión respectiva no deberá ser mayor a los quince días útiles de recibido el presente documento. Asimismo, Su opinión será de valioso aporte a la comisión que presido, coadyuvando al resultado de este, por lo que agradeceré sus importantes comentarios a la brevedad posible.

El proyecto de ley mencionado para estudio y análisis por su institución podrá ser descargado en el siguiente link: [pdf](#)

Hago propicia la ocasión para testimoniarle las muestras de mi especial consideración y estima personal.

Atentamente,



Firmado digitalmente por:
ORÚ MEDINA Ariana Maybee
FAU 20181749126 soft
Motivo: Soy el autor del
documento
Fecha: 22/01/2026 08:50:52-0500

ARIANA MAYBEE ORÚ MEDINA
Presidenta
Comisión de Ciencia, Innovación y Tecnología

AMOM/ica

Lima, 20 de enero de 2026

OFICIO N° 00155 - PO - 2025 - 2026-CCIT-AMOM-CR

Señor
JORGE EDUARDO FIGUEROA GUZMÁN
Ministro de Educación (MINEDU)
Calle El Comercio N° 193
San Borja.-

De mi consideración:

Es grato dirigirme a usted para saludarlo cordialmente, y en la oportunidad solicitar se sirva remitir opinión técnico legal y/o sugerencias, respecto del **Proyecto de Ley 13511-2025-CR, PROPONE DECLARAR EL DÍA NACIONAL DE LA SEGURIDAD INFORMÁTICA – CIBERSEGURIDAD, CON LA FINALIDAD DE QUE EL ESTADO CONCIENTICE A LAS PERSONAS Y ORGANIZACIONES LA IMPORTANCIA DE EJERCER BUENAS PRÁCTICAS DE SEGURIDAD AL UTILIZAR COMPUTADORAS, INTERNET, O CUALQUIER OTRO MEDIO DE ALMACENAMIENTO DE INFORMACIÓN.**

Este pedido se formula, al amparo de lo dispuesto en el artículo 96 de la Constitución Política del Perú, y en los artículos 22, literal b), 69 y 87 del Reglamento del Congreso de la República.

El plazo para la remisión de la opinión respectiva no deberá ser mayor a los quince días útiles de recibido el presente documento. Asimismo, Su opinión será de valioso aporte a la comisión que presido, coadyuvando al resultado de este, por lo que agradeceré sus importantes comentarios a la brevedad posible.

El proyecto de ley mencionado para estudio y análisis por su institución podrá ser descargado en el siguiente link: <https://api.congreso.gob.pe/spley-portal-service/archivo/MzU2NjYw/pdf>

Hago propicia la ocasión para testimoniarle las muestras de mi especial consideración y estima personal.

Atentamente,



Firmado digitalmente por:
ORUÉ MEDINA Ariana Maybee
FAU 20181749126 soft
Motivo: Soy el autor del
documento
Fecha: 22/01/2026 06:54:21-0500

ARIANA MAYBEE ORUÉ MEDINA
Presidenta
Comisión de Ciencia, Innovación y Tecnología

AMOM/ica



PROYECTO DE LEY QUE DECLARA EL 3 DE DICIEMBRE DE CADA AÑO, COMO EL “DÍA NACIONAL DE LA CIBERSEGURIDAD”

El congresista de la república **ALFREDO PARIONA SINCHE**, miembro de la BANCADA SOCIALISTA, ejerciendo el derecho de iniciativa legislativa que le confiere el artículo 107 de la Constitución Política del Perú y en concordancia con los artículos 22 inciso c) 67, 75 y 76 del reglamento del Congreso de la República presenta el siguiente proyecto de ley.

FÓRMULA LEGAL

El Congreso de la República,
Ha dado la ley siguiente:

LEY QUE DECLARA EL 3 DE DICIEMBRE DE CADA AÑO, COMO EL “DÍA NACIONAL DE LA CIBERSEGURIDAD”

Artículo 1. Objeto de la ley

La presente ley tiene por objeto declarar el día 3 de diciembre de cada año, como el “Día Nacional de la Ciberseguridad”, con el propósito de promover la protección de los datos personales, la integridad de las infraestructuras digitales y, la confianza en el uso de las tecnologías de la información y la comunicación (TIC), a fin de concientizar, fortalecer las capacidades técnicas y educativas, fomentar la cooperación público-privada y, fomentar la investigación y la innovación en materia de ciberseguridad.

Artículo 2. Declaratoria

Se declara el día 3 de diciembre de cada año, como el “Día Nacional de la Ciberseguridad”.

Artículo 3. Implementación

La Presidencia del Consejo de Ministros (PCM), a través de la Secretaría de Gobierno y Transformación Digital, coordina con los ministerios, así como, con los sectores público y privado, la realización de las siguientes acciones:

- a) Campañas nacionales de sensibilización sobre buenas prácticas digitales.
- b) Simulacros nacionales de ciberataques orientados a mejorar la capacidad de respuesta institucional.

- c) Programas educativos en coordinación con el Ministerio de Educación (Minedu) y la Autoridad Nacional del Servicio Civil (Servir), para incluir contenidos de ciberseguridad en todos los niveles de enseñanza y capacitación pública.
- d) Reconocimiento anual “Perú Ciberseguro”, a las instituciones que demuestren buenas prácticas y políticas efectivas de ciberseguridad.

Artículo 4. Participación interinstitucional

Las entidades públicas, empresas privadas, universidades y, organizaciones civiles participarán en las actividades del “Día Nacional de la Ciberseguridad”, en el marco de la Política Nacional de Transformación Digital.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. La Secretaría de Gobierno y Transformación Digital, en coordinación con la Presidencia del Consejo de Ministros (PCM), emitirá las directivas necesarias para la ejecución de la presente Ley, en un plazo no mayor de noventa (90) días calendario.

SEGUNDA. El Ministerio de Educación (Minedu), adoptara las acciones que correspondan, a efectos de que se incorpore contenidos de ciberseguridad en el currículo escolar.

TERCERA. La Autoridad Nacional del Servicio Civil (Servir) y, la Escuela Nacional de Administración Pública (ENAP), incluirán un módulo obligatorio de ciberseguridad en su formación continua para servidores públicos.

CUARTA. El Ministerio de Economía y Finanzas (MEF), adoptará las acciones que correspondan, a efectos de que se promueva certificaciones nacionales bajo estándares ISO 27001 y NIST CSF en instituciones críticas del Estado.

Lima, diciembre de 2025



Firmado digitalmente por:
PARIONA SINCHE Alfredo
FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 01/12/2025 14:48:13-0500

ALFREDO PARIONA SINCHE
Congresista de la República



Firmado digitalmente por:
DAVILA ATANACIO Pasion
Neomias FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 01/12/2025 15:03:18-0500



Firmado digitalmente por:
QUITO SARMIENTO Bernardo
Jaime FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 01/12/2025 15:49:34-0500



Firmado digitalmente por:
ROBLES ARAUJO Silvana
Emperatriz FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 01/12/2025 16:35:18-0500



Firmado digitalmente por:
FLORES RAMIREZ Alex Randu
FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 01/12/2025 16:58:59-0500



Firmado digitalmente por:
DAVILA ATANACIO Pasion
Neomias FAU 20161749126 soft
Motivo: Soy el autor del documento
Fecha: 01/12/2025 15:02:58-0500

EXPOSICIÓN DE MOTIVOS

FUNDAMENTACIÓN DE LA PROPUESTA:

El numeral 6 del artículo 2 de la Constitución Política del Perú, establece que, *“Toda persona tiene derecho: [...] 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar [...]”*.

Además, el artículo 14-A de la Constitución Política del Perú, señala que, *“El Estado garantiza, a través de la inversión pública o privada, el acceso a internet libre en todo el territorio nacional, con especial énfasis en las zonas rurales, comunidades campesinas y nativas.”*

El artículo 16 de la Ley 29733, Ley de protección de datos personales, indica que, *“Para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado. Los requisitos y condiciones que deben reunir los bancos de datos personales en materia de seguridad son establecidos por la Autoridad Nacional de Protección de Datos Personales, salvo la existencia de disposiciones especiales contenidas en otras leyes. Queda prohibido el tratamiento de datos personales en bancos de datos que no reúnan los requisitos y las condiciones de seguridad a que se refiere este artículo.”*

Además, el artículo 17 de la Ley 29733, Ley de protección de datos personales, señala que, *“El titular del banco de datos personales, el encargado y quienes intervengan en cualquier parte de su tratamiento están obligados a guardar confidencialidad respecto de los mismos y de sus antecedentes. Esta obligación subsiste aun después de finalizadas las relaciones con el titular del banco de datos personales. El obligado puede ser relevado de la obligación de*

confidencialidad cuando medie consentimiento previo, informado, expreso e inequívoco del titular de los datos personales, resolución judicial consentida o ejecutoriada, o cuando medien razones fundadas relativas a la defensa nacional, seguridad pública o la sanidad pública, sin perjuicio del derecho a guardar el secreto profesional.”

El artículo 2 de la Ley 30096, Ley de Delitos Informáticos, establece que, *“El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, o se excede en lo autorizado, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Si el agente accede deliberada e ilegítimamente, en todo o en parte, al sistema informático vulnerando las medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.”*

De igual modo, el artículo 8 de la Ley 30096, Ley de Delitos Informáticos, señala que, *“El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos, suplantación de interfaces o páginas web o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años y con sesenta a ciento veinte días-multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social. La misma pena se aplica al que intencionalmente colabora con la comisión de alguno de los supuestos de los párrafos precedentes, facilitando la transferencia de activos.”*

El artículo 1 de la Ley 30999, Ley de Ciberdefensa, dispone que, *“La presente ley tiene por objeto establecer el marco normativo en materia de ciberdefensa del Estado peruano, regulando las operaciones militares en y mediante el*

ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforme a ley.”

El artículo 3 del Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, establece las siguientes definiciones, “[...] g) *Riesgo de seguridad digital.- Efecto de la incertidumbre relacionada con el uso, desarrollo y gestión de las tecnologías digitales y datos, en el curso de cualquier actividad. Resulta de la combinación de amenazas y vulnerabilidades en el entorno digital y es de naturaleza dinámica. Puede socavar el logro de los objetivos económicos y sociales al alterar la confidencialidad, integridad y disponibilidad de las actividades o el entorno, así como poner en riesgo la protección de la vida privada de las personas. Incluye aspectos relacionados con los entornos físicos y digitales, las actividades críticas, las personas y organizaciones involucradas en la actividad y los procesos organizacionales que la respaldan. h) Ciberseguridad.- Capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital. Comprende la perspectiva técnica de la Seguridad Digital y es un ámbito del Marco de Seguridad Digital del país [...].”*

Además, el artículo 7 del Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, indica que, “7.1 *Créase el Centro Nacional de Seguridad Digital como una plataforma digital que gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer la confianza digital. Asimismo, es responsable de identificar, proteger, detectar, responder, recuperar y recopilar información sobre incidentes de seguridad digital en el ámbito nacional para gestionarlos. 7.2 El Centro Nacional de Seguridad Digital se encuentra a cargo de la Presidencia del*

Consejo de Ministros, a través de la Secretaría de Gobierno Digital, y es el único punto de contacto nacional en las comunicaciones y coordinaciones con otros organismos, centros o equipos nacionales e internacionales de similar naturaleza. 7.3 El Centro Nacional de Seguridad Digital constituye el mecanismo de intercambio de información y articulación de acciones con los responsables de los ámbitos del Marco de Seguridad Digital del Estado Peruano, de conformidad con el artículo 32 del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital. 7.4 El Centro Nacional de Seguridad Digital incorpora al Equipo de Respuesta a Incidentes de Seguridad Digital Nacional responsable de: i) Gestionar la respuesta y/o recuperación ante incidentes de seguridad digital en el ámbito nacional y, ii) Coordinar y articular acciones con otros equipos de similar naturaleza nacionales e internacionales para atender los incidentes de seguridad digital 7.5 La Secretaría de Gobierno Digital establece los protocolos de escalamiento, coordinación, intercambio y activación ante incidentes de seguridad digital en el país y emite los lineamientos y las directivas correspondientes.”

“La Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, es responsable del gobierno, gestión, promoción e impulso, para dictar políticas y estrategias en materia de transformación digital para el uso y aprovechamiento de la Red Nacional del Estado Peruano (REDNACE) y la Red Nacional de Investigación y Educación (RNIE), para lo cual dicta las normas para su adecuado funcionamiento y coordina su implementación con las entidades correspondientes.”¹

“El Ministerio de Transportes y Comunicaciones, a través del Programa Nacional de Telecomunicaciones - PRONATEL, es el responsable de implementar, mantener, operar y supervisar la infraestructura de la Red Nacional del Estado Peruano (REDNACE), así como de desplegar la infraestructura de última milla

¹ Decreto de Urgencia 007-2020. Tercera Disposición Complementaria Final.
LINK: <https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1252588>

para instituciones públicas, para dicho fin, el Ministerio de Transportes y Comunicaciones, dicta normas y coordina su operación con las entidades correspondientes, de conformidad con lo establecido en la Ley N° 29904, Ley de Promoción de la Banda Ancha y construcción de la Red Dorsal Nacional de Fibra Óptica y su reglamento.”²

“La norma ISO/IEC 27001 es el estándar internacional para sistemas de gestión de seguridad de la información (SGSI) de mejores prácticas. Es una especificación rigurosa y completa para proteger y preservar su información bajo los principios de confidencialidad, integridad y disponibilidad. La Norma ofrece un conjunto de controles de mejores prácticas que pueden aplicarse a su organización en función de los riesgos que enfrenta e implementarse de manera estructurada para lograr un cumplimiento certificado y evaluado externamente. El estándar también se puede ampliar integrándolo con varios otros estándares y marcos, incluidos NIST CSF (Marco de ciberseguridad) y NIST RMF (Marco de gestión de riesgos).”³

“El 30 de noviembre se celebra en todo el mundo el “Día de la Ciberseguridad” con el objetivo de concienciar sobre los riesgos que se esconden en la red y la importancia de proteger la información digital en un contexto en el que el ciberdelito aumenta año a año y es cada vez más sofisticado. La fecha se instauró en 1988 por iniciativa de la Association for Computing Machinery (ACM), cuando se detectó el primer caso de malware (software malicioso) de propagación en red del mundo.”⁴

² Decreto de Urgencia 007-2020. Tercera Disposición Complementaria Final.
LINK: <https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1252588>

³ ISO 27001 y el NIST CSF (Marco de Ciberseguridad)
LINK: <https://www-itgovernanceusa-com.translate.goog/iso27001-and-nist? x tr sl=en& x tr tl=es& x tr hl=es& x tr pto=tc>

⁴ Santander. 30 de noviembre: Día Mundial de la ciberseguridad. 30 de noviembre de 2022.
LINK: <https://www.santanderconsumer.es/simplefinance/blog/tu-futuro/ciberseguridad/post/30-de-noviembre-dia-mundial-de-la-ciberseguridad>

“El 3 y 4 de diciembre, se celebra la “Cumbre de ciberamenazas SANS 2025”, en el que se reúne la comunidad europea de ciberseguridad. Diseñado para profesionales de la seguridad, este evento abarca disciplinas tanto ofensivas como defensivas, con un enfoque especial en los aspectos técnicos. Ofrece un valor excepcional a profesionales de la ciberseguridad de todos los niveles, ofreciendo un entorno donde pueden compartir experiencias, conocimientos, herramientas y técnicas para impulsar el progreso en este campo. CyberThreat tiene como objetivo ofrecer la mejor conferencia técnica de Europa para profesionales de la ciberseguridad.”⁵

Además, según la ONU, “el 3 de diciembre se celebra el Día Internacional de las Personas con Discapacidad, por el que, se planteó la Estrategia de las Naciones Unidas para la Inclusión de la Discapacidad, acorde con su compromiso de hacer que las Naciones Unidas sean una organización inclusiva para todos, la cual constituye la base de un progreso sostenible y transformador hacia la inclusión de la discapacidad en todos los pilares de la labor de la ONU.”⁶ Lo cual refuerza el principio de accesibilidad y seguridad digital inclusiva, toda vez que, la ciberseguridad no solo protege sistemas, sino también a las personas más vulnerables en el entorno digital.

De igual forma, teniendo coherencia con el ecosistema internacional de derechos digitales, diciembre también es un mes simbólico en materia de derechos digitales, pues el 10 de diciembre se celebra el Día Internacional de los Derechos Humanos, cuyo principio de protección de la privacidad digital se encuentra directamente vinculado con la ciberseguridad.

⁵ SANS. Cumbre de ciberamenazas SANS 2025.

LINK: <https://www.sans.org/cyber-security-training-events/cyberthreat-2025>

⁶ ONU. Día Internacional de las Personas con Discapacidad 3 de diciembre.

LINK: <https://www.un.org/es/observances/day-of-persons-with-disabilities>

En la era digital, la ciberseguridad se ha convertido en un componente esencial de la soberanía nacional, la protección de los derechos fundamentales y la estabilidad económica. El Perú, al igual que el resto del mundo, enfrenta crecientes desafíos derivados del cibercrimen, el espionaje digital y la desinformación automatizada. Según el CERT-PERÚ (2024), se registraron más de 22,000 incidentes cibernéticos, afectando tanto a instituciones públicas como privadas. Además, ASBANC estima pérdidas anuales superiores a S/ 3,800 millones por fraudes digitales, y el 60% de usuarios peruanos aún no utiliza autenticación en dos pasos. Estas cifras reflejan una urgente necesidad de concientizar y educar a la población en prácticas seguras en línea.

En tal sentido, en atención a la convergencia internacional, se propone el 3 de diciembre, en armonía con los marcos de cooperación iberoamericana e internacional en materia de ciberseguridad, impulsados por organismos como la SEGIB, la OEI, la UIT y la OEA, pues durante este periodo (noviembre–diciembre) se desarrollan anualmente actividades, informes y foros regionales sobre seguridad digital, que permiten al Perú sincronizar sus esfuerzos de política pública con las tendencias globales y promover la integración regional en materia de confianza digital y soberanía tecnológica.

EFFECTOS DE LA VIGENCIA DE LA NORMA EN LA LEGISLACIÓN NACIONAL

La vigencia de la presente Ley no contraviene ninguna normativa y se encuentra acorde de los artículos 2, 14-A y, numeral 1 del artículo 102 de la Constitución Política del Perú, puesto que, se propone se declare el día 3 de diciembre de cada año, como el “Día Nacional de la Ciberseguridad”, con el propósito de promover la protección de los datos personales, la integridad de las infraestructuras digitales y, la confianza en el uso de las tecnologías de la información y la comunicación (TIC).

ANÁLISIS COSTO-BENEFICIO

La presente iniciativa legislativa no irroga gasto adicional al erario nacional, puesto que, es una propuesta declarativa que pretende que el día 3 de diciembre de cada año, como el “Día Nacional de la Ciberseguridad”, a fin de concientizar, fortalecer las capacidades técnicas y educativas, fomentar la cooperación público-privada y, fomentar la investigación y la innovación en materia de ciberseguridad.

Además, cabe precisar que, diciembre marca el cierre del año académico y presupuestal, lo que facilita la evaluación de políticas públicas en materia de transformación digital y permite proyectar planes de ciber formación para el siguiente año escolar y fiscal. Así, el “Día Nacional de la Ciberseguridad” se convierte en un espacio de balance, reflexión y planificación nacional, por lo que, resulta muy beneficioso para promover una cultura preventiva digital entre ciudadanos, empresas y el Estado, incluso conllevará a fortalecer las capacidades técnicas y la conciencia pública sobre los riesgos cibernéticos; y, establecer un espacio institucional para la coordinación intersectorial en materia de ciberseguridad.

RELACIÓN CON LAS POLÍTICAS DE ESTADO EXPRESADAS EN EL ACUERDO NACIONAL

El Proyecto de Ley tiene vinculación directa con la **Novena Política de Estado del Acuerdo Nacional**: “Política de seguridad nacional”, en la cual se establece que, nos comprometemos a mantener una política de seguridad nacional que garantice la independencia, soberanía, integridad territorial y la salvaguarda de los intereses nacionales. Consideramos que ésta es una tarea que involucra a la sociedad en su conjunto, a los organismos de conducción del Estado, en especial a las Fuerzas Armadas, en el marco de la Constitución y las leyes. En tal sentido, nos comprometemos a prevenir y afrontar cualquier amenaza externa o interna que ponga en peligro la paz social, la seguridad integral y el bienestar general. [...]”

Además, guarda relación con la **Vigésimo Política de Estado del Acuerdo Nacional**: “Desarrollo de la ciencia y la tecnología”, en la cual se establece que, nos comprometemos a fortalecer la capacidad del país para generar y utilizar conocimientos científicos y tecnológicos, para desarrollar los recursos humanos y para mejorar la gestión de los recursos naturales y la competitividad de las empresas. De igual manera, nos comprometemos a incrementar las actividades de investigación y el control de los resultados obtenidos, evaluándolos debida y puntualmente. Nos comprometemos también a asignar mayores recursos financieros mediante concursos públicos de méritos que conduzcan a la selección de los mejores investigadores y proyectos, así como a proteger la propiedad intelectual [...]”

Lima, diciembre de 2025